(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 532 228 A3**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **92308000.6**

(51) Int. Cl.[5] : **H04L 9/32**, H04L 9/06

(22) Date of filing : **03.09.92**

(30) Priority : **13.09.91 US 759309**

(43) Date of publication of application :
17.03.93 Bulletin 93/11

(84) Designated Contracting States :
DE FR GB SE

(88) Date of deferred publication of search report :
13.04.94 Bulletin 94/15

(71) Applicant : **AMERICAN TELEPHONE AND TELEGRAPH COMPANY**
32 Avenue of the Americas
New York, NY 10013-2412 (US)

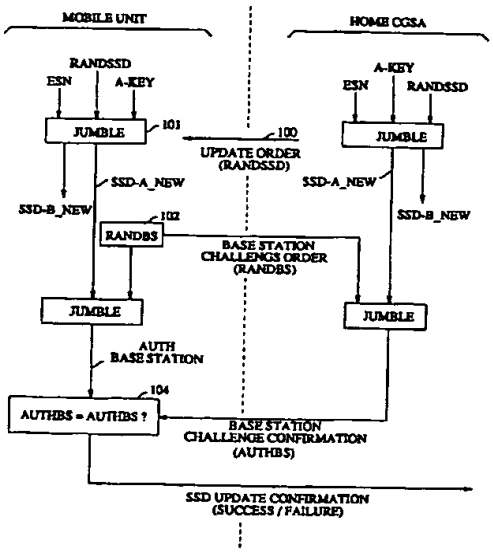
(72) Inventor : **Reeds III, James Alexander**
127 Southgate Road
New Providence, New Jersey 07974 (US)

(74) Representative : **Buckley, Christopher Simon Thirsk et al**
AT & T (UK) LTD., AT & T Intellectual Property Division, 5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) A cryptosystem for cellular telephony.

(57) A relatively secure, self-inverting, symmetric key cryptosystem designed for efficient implementation on an 8-bit microcomputer. The cryptosystem is especially well suited use in cellular telephony. The method of encryption is comprised of three stages : 1) an autokeyed encryption, 2) the use of a one-time pad encryption where the key is derived from a portion of the message as encrypted by the fist stage, and 3) a second autokeyed decryption that is the inverse of the fist.

FIG. 2



EP 0 532 228 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 92 30 8000

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
X	EP-A-0 105 553 (STAAT DER NEDERLANDEN) * page 4, line 11 - line 20 *	1,12	H04L9/32 H04L9/06
D,A	PROCEEDINGS OF THE IEEE vol. 67, no. 3 , March 1979 , NEW YORK US pages 397 - 427 W.DIFFIE ET AL 'PRIVACY AND AUTHENTICATION: AN INTRODUCTION TO CRYPTOGRAPHY' * page 412, left column, last paragraph *	2,13	

TECHNICAL FIELDS SEARCHED (Int.Cl.5)

H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	14 February 1994	Holper, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)